



מדריך לניהול שולחן העבודה

מחשבים שולחניים עסקיים

מק"ט מסמך: 312947-BB2

ספטמבר 2003

מדריך זה מספק הגדרות והוראות לשימוש בתכונות האבטחה והניהול הנבון שהותקנו מראש בדגמים נבחרים.

© 2003 כל הזכויות שמורות לחברת Hewlett-Packard Development, L.P.
HP, Hewlett Packard והלוגו של Hewlett Packard הם סימנים מסחריים של
חברת Hewlett Packard בארה"ב ובמדינות אחרות.

קומפאק והלוגו של קומפאק הם סימנים מסחריים רשומים של חברת
Hewlett Packard בארה"ב ובמדינות אחרות.
מיקרוסופט, MS-DOS, חלונות וחלונות NT הם סימנים מסחריים של חברת
מיקרוסופט בארה"ב ובמדינות אחרות.

ייתכן כי שמות מוצרים אחרים המוזכרים במסמך זה הם סימנים מסחריים
של החברות בהתאמה.

חברת Hewlett-Packard לא תישא בכל אחריות שהיא לשגיאות טכניות או
לשגיאות עריכה או להשמטות במסמך זה או לנזקים נסיבתיים או מקריים
הקשורים ליישום, לביצועים או לשימוש של חומר זה. המידע במסמך זה
מופיע "כמות שהוא", ללא אחריות כלשהי, לרבות האחריות המשתמעת של
סחירות והתאמה לשימוש מסוים, והוא נתון לשינויים ללא חובת הודעה
מראש. כתבי האחריות החלים על מוצרי HP מפורטים במפורש בכתבי
האחריות המוגבלת הנלווים למוצרים אלה. אין להבין מתוך הכתוב לעיל כי
תחול על המוצר אחריות נוספת כלשהי.

מסמך זה מכיל נתוני בעלות המעוגנים בזכויות יוצרים. אין להעתיק, לשכפל
או לתרגם לשפה אחרת חלקים כלשהם ממסמך זה ללא אישור מראש
ובכתב מחברת Hewlett-Packard.

אזהרה: טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום
לנזק גופני חמור ואף למוות.



זהירות: טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום
נזק לצידוד, וכן לאובדן נתונים או מידע.



מדריך לניהול שולחן העבודה
מחשבים שולחניים עסקיים
מהדורה שנייה (ספטמבר 2003)
מק"ט מסמך: 312947-BB2

תוכן עניינים

מדריך לניהול שולחן העבודה

2	הגדרת תצורה ראשונית ופריסה
3	התקנת מערכת מרחוק
4	עדכון וניהול תוכנות
4	HP Client Manager Software (תוכנה לניהול לקוחות של HP)
4	Altiris Solutions
5	Altiris PC Transplant Pro
6	מנהל תוכנת המערכת
6	Proactive Change Notification (דיווח מראש על שינויים)
6	ActiveUpdate (תוכנת עדכון פעיל)
7	זיכרון הבזק ROM
7	Remote ROM Flash (זיכרון הבזק ROM מרחוק)
8	HPQFlash
8	FailSafe Boot Block ROM
10	שכפול ההגדרות
19	לחצן הפעלה דו-מצבי
20	אתר האינטרנט
20	אבני בניין ושותפים
21	בקרת נכסים ואבטחה
25	אבטחה באמצעות סיסמה
25	קביעת סיסמת הגדרות באמצעות הגדרות המחשב
26	קביעת סיסמת הפעלה (Power-On) באמצעות הגדרות המחשב
30	אבטחה משובצת (Embedded Security)
39	DriveLock
41	Smart Cover Sensor (חיישן המכסה החכם)
42	Smart Cover Lock (מנעול המכסה החכם)
45	Master Boot Record Security (אבטחת רשומת אתחול ראשית)
47	לפני הגדרת מחיצות או ביצוע פורמט של דיסק האתחול הנוכחי
47	Cable Lock Provision (התקן מנעול כבל)

48	טכנולוגיה לזיהוי טביעות אצבעות
48	הודעות כשל והתאוששות
48	Drive Protection System (מערכת להגנה על כוננים)
49	עמידה בנחשולי מתח
49	חיישן תרמי

אינדקס

מדריך לניהול שולחן העבודה

ניהול נבון של HP מספק פתרונות המבוססים על סטנדרטים מקובלים לניהול ולבקרה על שולחנות עבודה, תחנות עבודה ומחשבי מחברת בסביבת רשת. בשנת 1995 הפכה חברת HP לחלוצה בכל הקשור ליכולת הניהול של שולחן העבודה, זאת הודות להשקעה של ראשוני המחשבים האישיים שתמכו ביכולת ניהול מלאה. חברת HP מחזיקה בפטנט על טכנולוגיית יכולת הניהול שלה. מאז הייתה חברת HP חברה מובילה בתעשייה במאמציה לפתח סטנדרטים ותשתית הדרושים לפריסה, להגדרות תצורה ולניהול של שולחנות עבודה, תחנות עבודה ומחשבי מחברת. HP פועלת בשיתוף פעולה הדוק עם ספקי פתרונות ניהול כדי להבטיח תאימות בין טכנולוגיית הניהול הנבון לבין מוצרים אלה. ניהול נבון מהווה נדבך חשוב בהתחייבות העמוקה שלנו לספק ללקוח פתרונות למשך כל מחזור החיים של המחשב, המסייעים במהלך ארבעת השלבים של תכנון, פריסה, ניהול והעברות.

להלן רשימת היכולות והתכונות המרכזיות של ניהול שולחן העבודה:

- הגדרת תצורה ראשונית ופריסה
- התקנת מערכת מרחוק
- עדכון וניהול תוכנה
- זיכרון הבזק ROM
- בקרת נכסים ואבטחה
- הודעות על מקרי כשל והתאוששות

תמיכה בתכונות ספציפיות המתוארות במדריך זה עלולה להשתנות לאור השוני בין דגמים וגרסאות תוכנה.



הגדרת תצורה ראשונית ופריסה

המחשב מגיע עם תמונת תוכנת מערכת (system software image) מותקנת מראש. לאחר תהליך קצר של "הוצאת התוכנה מהאריזה", יהיה המחשב מוכן לשימוש.

ייתכן שתעדיף להחליף את התוכנות המותקנות מראש בתוכנות מערכת ויישומים מותאמים אישית. קיימות מספר שיטות לפריסת תוכנות מותאמות אישית. שיטות אלה כוללות:

- התקנת יישומי תוכנה נוספים לאחר פתיחת תמונת התוכנה המותקנת מראש.

- שימוש בתוכנות פריסה, כגון Altiris Deployment Solution™, להחלפת התוכנות המותקנות מראש בתמונת תוכנה מותאמת אישית.

- שכפול דיסק קשיח לצורך העתקת התוכן מכונן קשיח אחד למשנהו.

שיטת הפריסה הטובה ביותר תלויה בסביבת טכנולוגית המידע שלך ובתהליכים שאתה משתמש בהם. סעיף PC Deployment (פריסת המחשב האישי) באתר HP Lifecycle Solutions

(<http://h18000.www1.hp.com/solutions/pc solutions>) מספק מידע

שיעזור לך לבחור את שיטת הפריסה הטובה ביותר.

תקליטור שחזור פלוס! ההגדרות מבוססות ה-ROM וחומרת ACPI מספקים סיוע נוסף בנוגע לשחזור תוכנות מערכת, ניהול תצורה, איתור תקלות וניהול צריכת חשמל.

התקנת מערכת מרחוק

התקנת המערכת מרחוק מאפשרת אתחול והגדרה של המערכת באמצעות שימוש בתוכנה ובנתוני הגדרת תצורה הנמצאים בשרת הרשת באמצעות הפעלת סביבת Preboot Execution Environment (PXE). תכונת התקנת המערכת מרחוק מופעלת בדרך כלל ככלי להתקנת והגדרת תצורת המערכת, וניתן להשתמש בה לביצוע המטלות הבאות:

- פירמוט דיסק קשיח
 - פריסת תמונת תוכנה במחשב אישי חדש אחד או יותר
 - עדכון מרחוק של BIOS המערכת בזיכרון הבזק ROM ("Remote ROM Flash" בעמוד 7)
 - קביעת תצורה של הגדרות BIOS המערכת
- כדי להתחיל בהתקנת מערכת מרחוק, הקש **F12** עם הופעת ההודעה F12 = Network Service Boot בפינה הימנית התחתונה של מסך הלוגו של HP. פעל על פי ההוראות המוצגות על המסך כדי להמשיך את התהליך. סדר האתחול המשמש כברירת מחדל הוא הגדרת תצורה של ה-BIOS, שניתן לשנותה לנסות תמיד לבצע אתחול PXE.
- HP ו-Altiris Inc. משתפות פעולה כדי לספק כלים, המיועדים להקל על משימת הפריסה של מחשבים ארגוניים ועל הניהול שלהם, לצמצם את הזמן הנדרש לצרכים ניהוליים אלה, להקטין בצורה קיצונית את עלויות הבעלות ולהפוך את המחשבים האישיים של HP למחשבי הלקוח המציעים את יכולות הניהול הטובות ביותר בסביבות ארגוניות.

עדכון וניהול תוכנות

HP מספקת מספר כלים לניהול ולעדכון התוכנה במחשבים שולחניים ובתחנות עבודה – Altiris PC Transplant Pro ; Altiris HP Client Manager ; Software, פתרון של Altiris ; System Software Manager ; Proactive Change ; Notification ; ו-ActiveUpdate.

HP Client Manager Software (תוכנה לניהול לקוחות של HP)

התוכנה המתוככמת (HP CMS) HP Client Manager Software משלבת בצורה הדוקה את טכנולוגיית הניהול הנבון של HP בתוך Altiris כדי לספק יכולות ניהול חומרה מעולות עבור התקני גישה של HP הכוללים :

- תצוגות מפורטות על מצאי החומרה לצורך ניהול נכסים
- בדיקות ניטור ואבחונים לגבי תקינות המחשב
- דיווח מראש לגבי שינויים בסביבת החומרה
- דיווחים דרך האינטרנט על פרטים עסקיים חשובים, כגון מחשבים עם אזהרות תרמיות, התראות זיכרון, ועוד
- עדכון מרחוק של תוכנת המערכת, כגון דרייברים להתקנים ו-ROM BIOS
- שינוי מרחוק של סדר האתחול
- לקבלת מידע נוסף, בקר באתר http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

תוכנת HP Client Management Solutions מאפשרת ניהול חומרה ריכוזי של התקני לקוח של HP עבור כל תחומי מחזור החיים של טכנולוגיית המידע.

- ניהול מצאי ונכסים
- תאימות לרשיון SW
- מעקב אחר המחשב ודיווח
- הסכם חכירה, תיקון בקרת נכסים
- פריסה והגירה
- הגירה לחלונות 2000, או לחלונות XP Professional או ל- Home Edition של מיקרוסופט

- ☐ פריסת מערכת
- ☐ הגירה אישית
- מרכז תמיכה ופתרון בעיות
- ☐ ניהול כרטיסי מרכז תמיכה
- ☐ איתור תקלות מרחוק
- ☐ פתרון בעיות מרחוק
- ☐ התאוששות מאסון של הלקוח
- ניהול תוכנה ופעילויות
- ☐ ניהול רציף של שולחן העבודה
- ☐ פריסת SW של מערכת HP
- ☐ החלמה עצמית של יישום

דגמים נבחרים של מחשבים שולחניים ומחשבי מחברת כוללים את סוכן הניהול של Altiris כחלק מהתמונה המותקנת על-ידי היצרן. סוכן זה מאפשר לנהל תקשורת עם Altiris Development Solution (פתרון הפיתוח של Altiris) שיכול לשמש להשלמת פריסת חומרה חדשה או הגירת אישיות למערכת הפעלה חדשה באמצעות אשפים נוחים לשימוש. הפתרונות של Altiris מספקים יכולות הפצת תוכנה נוחות לשימוש. כאשר משתמשים ביכולות אלה יחד עם מנהל תוכנת המערכת, או עם HP Client Manager, מנהלי מערכת יכולים גם לעדכן את ה-BIOS של זיכרון ROM ואת תוכנות הדרייברים של ההתקנים מתוך מסוף מרכזי.

לקבלת מידע נוסף, בקר באתר <http://www.hp.com/go/easydeploy>.

Altiris PC Transplant Pro

תוכנת Altiris PC Transplant Pro מאפשרת מעבר בין מחשבים אישיים תוך שמירה על הגדרות והעדפות קודמות ועל נתונים קודמים, והעברתם לסביבה החדשה במהירות ובקלות. פעולות השדרוג נמשכות דקות אחדות במקום שעות או ימים, ושולחן העבודה נראה ופועל בהתאם לציפיות המשתמשים. לקבלת מידע ופרטים נוספים אודות אופן ההורדה של גרסת הערכה למשך 30 יום, הכוללת את כל הפונקציות, בקר באתר <http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

מנהל תוכנת המערכת

מנהל תוכנת המערכת (SSM) הוא כלי עזר המאפשר לך לעדכן תוכנות ברמת המערכת במספר מחשבים בו-זמנית. כשמריצים את מנהל תוכנת המערכת במערכת של מחשבי לקוח, הוא מגלה הן את גרסת החומרה והן את גרסת התוכנה, ולאחר מכן מעדכן את התוכנה המתאימה באמצעות תוכנה הנלקחת מהארכיון המרכזי, הידוע גם כמחסן הקבצים. גרסאות דרייברים הנתמכות על-ידי SSM מצוינות בסמל מיוחד באתר הדרייברים ובתקליטור תוכנת התמיכה. להורדת כלי העזר, או לקבלת מידע נוסף בנושא SSM, בקר באתר <http://h18000.www1.hp.com/im/ssmwp.html>.

Proactive Change Notification (דיווח מראש על שינויים)

התוכנית Proactive Change Notification משתמשת באתר האינטרנט Subscriber's Choice כדי לבצע מראש ובאופן אוטומטי את הפעולות הבאות:

- שליחת הודעות דואר אלקטרוני של Proactive Change Notification (PCN) המדווחות על שינויים ברכיבי חומרה ותוכנה ברוב המחשבים והשרתים המסחריים, עד 60 ימים מראש.
- שליחת הודעות דואר אלקטרוני הכוללות עלונים ללקוח, דפי עזר, הערות ללקוח, עלוני אבטחה והתראות על דרייברים לרוב המחשבים והשרתים המסחריים.
- יצירת פרופיל אישי כדי להבטיח שרק אתה אישית תקבל את המידע הדרוש לסביבת טכנולוגיית מידע ספציפית. כדי ללמוד עוד אודות תוכנית Proactive Change Notification, וליצור פרופיל מותאם אישית, בקר בכתובת <http://www.hp.com/go/pcn>.

ActiveUpdate (תוכנת עדכון פעיל)

ActiveUpdate הוא יישום מבוסס-לקוח של HP. יישום הלקוח ActiveUpdate פועל במערכת המקומית, ומשתמש בפרופיל המוגדר על ידי המשתמש כדי להוריד מראש ובאופן אוטומטי עדכוני תוכנה לרוב המחשבים והשרתים המסחריים של HP. עדכוני תוכנה אלה שהורדת ניתנים לפריסה נבונה במחשבים שעבורם הם מיועדים על-ידי התוכנות HP Client Manager Software ו-System Software Manager. כדי ללמוד עוד אודות ActiveUpdate, להוריד את היישום, וליצור פרופיל מותאם אישית, בקר באתר http://h18000.www1.hp.com/products/servers/management/active_update/index.html

זיכרון הבזק ROM

המחשב האישי שלך כולל זיכרון הבזק ROM (זיכרון לקריאה בלבד) הניתן לתיכנות. על-ידי הגדרת סיסמת הגדרות בכלי העזר Computer Setup (F10) (הגדרות המחשב), תוכל להגן על זיכרון ה-ROM מפני עדכון או מפני דריסה בלתי מכוונת. הדבר חשוב כדי להבטיח את שלמות פעולתו של המחשב האישי. אם תרצה לשדרג את זיכרון ה-ROM, תוכל:

- להזמין תקליטון עם ROMPaq משודרג מ-HP.
- להוריד את תמונות ROMPaq העדכניות ביותר בכתובת <http://h18000.www1.hp.com/im/ssmwp.html>

זהירות: כדי לספק הגנה מרבית לזיכרון ROM, דאג להגדיר סיסמת הגדרות. סיסמת ההגדרות מונעת שדרוגים לא מורשים של זיכרון ROM. System Software Manager מאפשר למנהל המערכת להגדיר סיסמת הגדרות במחשב אישי אחד או במספר מחשבים אישיים בו-זמנית. לקבלת מידע נוסף, בקר באתר <http://h18000.www1.hp.com/im/ssmwp.html>



Remote ROM Flash (זיכרון הבזק ROM מרחוק)

Remote ROM Flash (זיכרון הבזק ROM מרחוק) מאפשר למנהל המערכת לשדרג בצורה בטוחה את זיכרון ROM במחשבי HP מרוחקים, ישירות מתוך עמדת ניהול רשת מרכזית. יכולתו של מנהל המערכת לבצע משימה זו מרחוק, במחשבים מרובים, מאפשרת פריסה עקבית ושליטה טובה יותר בתמונות זיכרון ROM במחשבי HP דרך הרשת. כמו כן, היא מאפשרת להגביר את התפוקה ולצמצם בעלויות הבעלות.

כדי לנצל את Remote ROM Flash, המחשב האישי צריך להיות דולק, או שיש להפעילו באמצעות יקיצה מרחוק (Remote Wakeup).



לקבלת מידע נוסף אודות Remote ROM Flash, עיין בתוכנות HP Client Manager Software או System Software Manager בכתובת <http://h18000.www1.hp.com/im/prodinfo.html>

HPQFlash

כלי העזר HPQFlash משמש לעדכון מקומי או לשחזור זיכרון מערכת במחשבים יחידים, באמצעות מערכת ההפעלה חלונות. לקבלת מידע נוסף אודות HPQFlash, בקר בכתובת <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html>

FailSafe Boot Block ROM

FailSafe Boot Block ROM מאפשר לבצע שחזור מערכת במקרים נדירים של כשל זיכרון ההבזק, למשל, אם התרחשה נפילת מתח בזמן שדרוג ROM. ה-Boot Block (בלוק אתחול) הוא אזור מוגן-הבזק של הזיכרון, המוודא את תקפות זיכרון ההבזק של המערכת עם התחלת אספקת המתח למערכת.

■ אם זיכרון המערכת תקין, המערכת מתחילה לפעול כרגיל.

■ אם זיכרון המערכת נכשל בבדיקות התקינות,


FailSafe Boot Block ROM מספק תמיכה מספקת לצורך אתחול המערכת מתקליטון ROMPaq, המתכנת את זיכרון המערכת לתצורה הרצויה.

כשתוכנת אתחול מזהה זיכרון מערכת לא תקף, נורת ההפעלה מהבהבת 8 פעמים בשנייה באור אדום, עם הפסקה של 2 שניות. כמו כן נשמעים 8 צפצופים ברציפות. הודעת שחזור של בלוק אתחול מופיעה על המסך (בדגמים מסוימים).

כדי לאפשר למערכת להתאושש, לאחר שזו נכנסת למצב Boot Block recovery, פעל על פי הצעדים הבאים:

1. אם יש תקליטון בכונן התקליטונים, הוצא אותו וכבה את המחשב.
2. הכנס את תקליטון ROMPaq לכונן התקליטונים.
3. הדלק את המחשב.
4. אם תקליטון ROMPaq לא נמצא, תתבקש להכניס תקליטון זה ולהפעיל מחדש את המחשב.
5. אם הוגדרה סיסמת הגדרות, נורת Caps Lock תידלק, ותתבקש להזין את הסיסמה.
6. הזן את סיסמת ההגדרות.

7. אם המערכת אותחלה בהצלחה מהתקליטון וביצעה בהצלחה תכנות מחדש של הזיכרון, שלוש הנורות שבמקלדת יידלקו. גם סדרה של צפצופים המתחזקים והולכים תציין את השלמת הפעולה בהצלחה.
 8. הוצא את התקליטון מכונן התקליטונים וכבה את המחשב.
 9. הדלק את המחשב ואתחל אותו.
- הטבלאות הבאות מציגות את צירופי הנורות השונים במקלדת המשמשים לצורך ROM בלוק האתחול (כשמקלדת PS/2 מחוברת למחשב), ומסבירות את המשמעות והפעולה הקשורות לכל צירוף כזה.

צירופי נורות מקלדת הנמצאים בשימוש על-ידי Boot Block ROM			
מצב/הודעה	פעולת נורות המקלדת	צבע נורות המקלדת	מצב FailSafe Boot Block
תקליטון ROMPaq לא נמצא, אינו תקין או שהכונן אינו מוכן.	דולקות	ירוק	Num Lock
הזן סיסמה.	דולקות	ירוק	Caps Lock
המקלדת נעולה במצב רשת.	מהבהבות בזו אחר זו, אחת בכל פעם – N, C, SL	ירוק	,Caps ,Num Scroll Lock
Boot Block ROM Flash הושלם בהצלחה. כבה את המחשב ולאחר מכן אתחל אותו.	דולקות	ירוק	,Caps ,Num Scroll Lock
נורות האבחון אינן נדלקות במקלדות USB. 			

שכפול ההגדרות

ההליכים הבאים מאפשרים למנהל המערכת יכולת להעתיק בקלות רבה תצורת הגדרות מערכת אחת למחשבים אישיים אחרים מאותו דגם. הדבר מאפשר לבצע הגדרת תצורה מהירה ועקבית של מחשבים מרובים.

שני ההליכים מחייבים כונן תקליטורים או התקן USB flash media נתמך, כגון HP Drive Key.



העתקה למחשב אחד

זהירות: תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההגדרות ממחשב D510 Ultra-slim Desktop למחשב D510 e-pc.



1. בחר תצורת הגדרות להעתקה. הדלק את המחשב או הפעל אותו מחדש. אם הנך עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.

2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. הכנס תקליטון התקן USB flash media.

4. לחץ על **File (קובץ) < Save to Diskette (שמור לתקליטון)**. בצע את ההוראות המוצגות על המסך כדי ליצור את תקליטון התצורה או את התקן USB flash media.

5. כבה את המחשב שיש להגדיר, והכנס את תקליטון התצורה או את התקן USB flash media.

6. הדלק את המחשב שיש להגדיר. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

7. לחץ על **File (קובץ) < Restore from Diskette (שחזר מתקליטון)** ולאחר מכן בצע את ההוראות המוצגות על המסך.

8. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

העתקה למחשבים מרובים

זהירות: תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההגדרות ממחשב D510 Ultra-slim Desktop למחשב D510 e-pc.



בשיטה זו דרוש מעט יותר זמן להכנת תקליטון התצורה או התקן USB flash media, אך העתקת התצורה למחשבי היעד מהירה יותר באופן משמעותי.

לא ניתן ליצור תקליטון בר-אתחול בחלונות 2000. תקליטון בר-אתחול דרוש להליך זה או ליצירת התקן USB flash media בר-אתחול. אם לא ניתן להשתמש בחלונות x9 או בחלונות XP ליצירת תקליטון בר-אתחול, השתמש בשיטה להעתקה למחשב אחד (ראה "העתקה למחשב אחד" בעמוד 10).



1. צור תקליטון בר-אתחול או התקן USB flash media. ראה "תקליטון בר-אתחול" בעמוד 12, "התקני USB Flash Media נתמכים" בעמוד 13, או "התקני USB Flash Media שאינם נתמכים" בעמוד 16.

זהירות: לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם תדר האתחול בכלי העזר (F10) Computer Setup (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחול את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון בר-אתחול.



2. בחר תצורת הגדרות להעתקה. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוש' < 'הפעל את המחשב מחדש'.

3. הקש על מקש F10 ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש Enter כדי לעקוף את מסך הפתיחה.

אם לא הקשת F10 בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש F10 כדי לגשת לכלי העזר.



4. הכנס את התקליטון בר-האתחול, או את התקן USB flash media.
5. לחץ על **File (קובץ) < Save to Diskette (שמור לתקליטון)**. בצע את ההוראות המוצגות על המסך כדי ליצור את תקליטון התצורה או את התקן USB flash media.
6. הורד כלי עזר של BIOS לשכפול ההגדרות (repset.exe) והעתק אותו לתקליטון התצורה או להתקן USB flash media. כלי עזר זה נמצא בכתובת <http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html>
7. בתקליטון התצורה או בהתקן USB flash media, צור קובץ autoexec.bat שמכיל את הפקודה הבאה:
repset.exe
8. כבה את המחשב שיש להגדיר. הכנס את תקליטון התצורה, או את התקן USB flash media, והדלק את המחשב. כלי העזר של התצורה יופעל באופן אוטומטי.
9. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

יצירת התקן בר-אתחול

תקליטון בר-אתחול

הוראות אלה מתאימות לחלונות XP ול-Home Edition. מערכת ההפעלה חלונות 2000 אינה תומכת ביצירת תקליטונים ברי-אתחול.



1. הכנס תקליטון לכוון התקליטונים.
 2. לחץ על **'התחל'**, ולאחר מכן לחץ על **'המחשב שלי'**.
 3. לחץ באמצעות לחצן העכבר הימני על כוון התקליטונים, ולאחר מכן לחץ על **'אתחול'**.
 4. בחר בתיבת הסימון **'צור דיסק הפעלה של MS-DOS'**, ולאחר מכן לחץ על **'התחל'**.
- חזור לסעיף "העתקה למחשבים מרובים" בעמוד 11.

התקני USB Flash Media נתמכים

התקנים נתמכים, כגון HP Drive Key או DiskOnKey, כוללים תמונה מותקנת מראש, כדי לפשט את תהליך הפיכתם לברי-אתחול. אם התקן Drive Key שנמצא בשימוש אינו כולל תמונה זו, השתמש בהליך המתואר בהמשך סעיף זה (ראה "התקני USB Flash Media שאינם נתמכים" בעמוד 16).

זהירות: לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בכלי העזר (F10) Computer Setup (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחל את המחשב מהתקן USB flash media. אחרת, יש להשתמש בתקליטון בר-אתחול.



כדי ליצור התקן USB flash media בר-אתחול, דרושים לך:

■ אחת מהמערכות הבאות:

- ☐ Compaq Evo D510 Ultra-slim Desktop
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor
- ☐ Ultra-slim Desktop, - HP Compaq Business Desktop d530 Series Convertible Minitower או Small Form Factor
- ☐ מחשבי מחברת מדגם Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c או N1000c

☐ מחשבי המחברת Compaq Presario 1500 או 2800

בהתאם ל-BIOS של כל מחשב, ייתכן שמערכות עתידיות יתמכו אף הן באתחול מהתקן HP Drive Key.

זהירות: אם אתה משתמש במחשב שונה מאלה המפורטים לעיל, ודא כי סדר האתחול המוגדר כברירת מחדל בכלי העזר (F10) Computer Setup (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח.



■ אחת ממודולי האחסון הבאים:

- ☐ 16MB HP Drive Key
- ☐ 32MB HP Drive Key
- ☐ 32MB DiskOnKey
- ☐ 64MB HP Drive Key
- ☐ 64MB DiskOnKey

128MB HP Drive Key ☐128MB DiskOnKey ☐

■ תקליטון DOS בר-אתחול עם התוכניות FDISK ו-SYS. אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים ב-Drive Key יאבדו.

1. כבה את המחשב.
2. הכנס את Drive Key לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB.
3. הכנס תקליטון בר-אתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכונן תקליטונים והדלק את המחשב כדי לבצע אתחול מתקליטון ה-DOS.
4. הפעל את FDISK מתוך שורת הפקודה A:\ על-ידי הקלדת **FDISK** והקשה על Enter. אם תבקש, לחץ על **Yes (Y)** כדי להפעיל תמיכה בדיסקים גדולים.
5. בחר באפשרות [5] כדי להציג את הכוננים במערכת. כונן Drive Key יהיה הכונן שגודלו קרוב ביותר לגודל של אחד הכוננים המוצגים. בדרך כלל זה יהיה הכונן האחרון ברשימה. שים לב לאות הכונן.
כונן Drive Key : _____

זהירות: אם כונן אינו תואם ל-Drive Key, אל תמשיך. במקרה כזה אתה עלול לאבד נתונים. חפש התקני אחסון נוספים בכל יציאות ה-USB. אם תאתר התקנים כאלה, הפעל את המחשב מחדש והמשך משלב 4. אם לא תמצא אף התקן, ייתכן שהמערכת אינה תומכת ב-Drive Key, או ש-Drive Key פגום. **אין** להמשיך ולנסות להפוך את Drive Key לבר-אתחול.



6. צא מ-FDISK על-ידי הקשה על מקש **Esc** כדי לחזור לשורת הפקודה A:\.
7. אם תקליטון DOS בר-האתחול מכיל את SYS.COM, עבור לשלב 8. אחרת, עבור לשלב 9.
8. בשורת הפקודה A:\, הזן **SYS x**. כאשר x מייצג את אות הכונן שצוינה לעיל. עבור לשלב 13.

זהירות: ודא שהזנת את אות הכונן הנכונה עבור Drive Key.



לאחר העברת קובצי המערכת, התוכנית SYS תחזור לשורת הפקודה A:\.

9. העתק קבצים שברצונך לשמור מכונן Drive Key לספרייה זמנית בכונן אחר (לדוגמה, הדיסק הקשיח הפנימי של המחשב).
10. בשורת הפקודה A:\, הזן **FORMAT /S X:**. כאשר x מייצג את אות הכונן שצוינה לפני כן.

זהירות: ודא שהזנת את אות הכונן הנכונה עבור Drive Key.



- התוכנית FORMAT תציג אזהרה אחת או יותר, ותשאל אותך בכל פעם אם ברצונך להמשיך. הקש y בכל פעם. התוכנית FORMAT תפרמט את Drive Key, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.
11. הקש **Enter** אם אינך מעוניין בתווית, או הזן תווית, אם רצונך בכך.
 12. העתק את הקבצים ששמרת בשלב 9 בחזרה ל-Drive Key.
 13. הוצא את התקליטון והפעל את המחשב מחדש. המחשב יבצע אתחול מ-Drive Key ככונן C.

סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בכלי העזר Computer Setup (F10) (הגדרות המחשב).



אם השתמשת בגירסת DOS מתוך חלונות 9x, ייתן שתראה את מסך הלוגו של חלונות למשך זמן קצר. אם אינך רואה מסך זה, הוסף קובץ באורך אפס בשם LOGO.SYS לספריית השורש של Drive Key.

חזור לסעיף "העתקה למחשבים מרובים" בעמוד 11.

התקני USB Flash Media שאינם נתמכים

זהירות: לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בכלי העזר (F10) Computer Setup (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחול את המחשב מהתקן USB flash media. אחרת, יש להשתמש בתקליטון בר-אתחול.



כדי ליצור התקן USB flash media בר-אתחול, דרושים לך:

■ אחת מהמערכות הבאות:

Compaq Evo D510 Ultra-slim Desktop ☐

Compaq Evo D510 Convertible Minitower/Small Form Factor ☐

Ultra-slim Desktop, - HP Compaq Business Desktop d530 Series ☐
Convertible Minitower או Small Form Factor

מחשבי מחברת מדגם Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c או N1000c ☐

מחשבי המחברת Compaq Presario 1500 או 2800 ☐

בהתאם ל-BIOS של כל מחשב, ייתכן שמערכות עתידיות יתמכו אף הן באתחול מהתקן USB flash media.

זהירות: אם אתה משתמש במחשב שונה מאלה המפורטים לעיל, ודא כי סדר האתחול המוגדר כברירת מחדל בכלי העזר (F10) Computer Setup (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח.



■ תקליטון DOS בר-אתחול עם התוכניות FDISK ו-SYS. אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים ב-Drive Key יאבדו.

1. אם קיימים כרטיסי PCI במערכת, שמחוברים אליהם כונני SCSI, ATA RAID או SATA, כבה את המחשב ונתק את חוט החשמל.

זהירות: חוט החשמל חייב להיות מנותק.



2. פתח את המחשב והוצא את כרטיסי ה-PCI.

3. הכנס את התקן USB flash media לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB. סגור את מכסה המחשב.

4. חבר את חוט החשמל והדלק את המחשב. ברגע שנורת הצג תהפוך לירוקה, הקש על מקש **F10** כדי להיכנס לכלי העזר Computer Setup (הגדרות המחשב).
5. עבור ל-Advanced/PCI devices (התקנים מתקדמים/התקני PCI) כדי להשבית את בקרי IDE ו-SATA. בעת השבתת בקר SATA, שים לב ל-IRQ שאליו מוקצה הבקר. יהיה עליך להקצות מחדש את ה-IRQ בשלב מאוחר יותר. יציאה מתוכנית ההגדרות מאשרת את השינויים.
SATA IRQ: _____
6. הכנס תקליטון בר-אתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכוון תקליטונים והדלק את המחשב כדי לבצע אתחול מתקליטון ה-DOS.
7. הפעל את FDISK ומחק מחיצות קיימות בהתקן USB flash media. צור מחיצה חדשה וסמן אותה כפעילה. צא מ-FDISK על-ידי הקשה על מקש **Esc**.
8. אם לא מתבצעת הפעלה מחדש של המערכת לאחר יציאה מ-FDISK, הקש **Ctrl+Alt+Del** כדי לבצע אתחול מתקליטון DOS.
9. בשורת הפקודה A:\, הזן **FORMAT C: /S** והקש **Enter**. התוכנית FORMAT תפרמט את התקן USB flash media, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.
10. הקש **Enter** אם אינך מעוניין בתווית, או הזן תווית, אם רצונך בכך.
11. כבה את המחשב ונתק את חוט החשמל. פתח את המחשב והתקן מחדש את כרטיסי PCI שהוצאת לפני כן. סגור את מכסה המחשב.
12. חבר את חוט החשמל, הוצא את התקליטון והדלק את המחשב.
13. ברגע שנורת הצג תהפוך לירוקה, הקש על מקש **F10** כדי להיכנס לכלי העזר Computer Setup (הגדרות המחשב).
14. עבור ל-Advanced/PCI Devices (התקנים מתקדמים/התקני PCI) והפעל מחדש את בקר IDE ו-SATA שהשבתת בשלב 5. הקצה לבקר SATA את ה-IRQ המקורי שלו.
15. שמור שינויים וצא. המחשב יבצע אתחול מהתקן USB flash media ככונן C.

סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בכלי העזר Computer Setup (F10) (הגדרות המחשב).



אם השתמשת בגירסת DOS מתוך חלונות 9x, ייתן שתראה את מסך הלוגו של חלונות למשך זמן קצר. אם אינך רוצה לראות מסך זה, הוסף קובץ באורך אפס בשם LOGO.SYS לספריית השורש של Drive Key.

חזור לסעיף "העתקה למחשבים מרובים" בעמוד 11.

לחצן הפעלה דו-מצבי

בעזרת ממשק התצורה והמתח המתקדם (ACPI) המופעל בחלונות 2000, חלונות XP Professional ו-Home Edition, יכול לחצן המתח לתפקד כלחצן הפעלה או כלחצן השעיה. תכונת ההשעיה אינה מנתקת לחלוטין את המתח מהמחשב, אלא גורמת לו להיכנס למצב המתנה תוך כדי צריכת מתח נמוכה. דבר זה מאפשר לך להוריד במהירות את צריכת המתח ללא סגירת היישומים, ולחזור במהירות למצב הפעלה רגיל מבלי לאבד נתונים.

כדי לשנות את תצורת לחצן ההפעלה, פעל לפי הצעדים הבאים:

1. בחלונות 2000, לחץ על לחצן '**התחל**', לאחר מכן בחר '**הגדרות**' < '**לוח הבקרה**' < '**אפשרויות צריכת חשמל**'.
בחלונות XP Professional ו-Home Edition, לחץ על לחצן '**התחל**', לאחר מכן בחר באפשרות '**לוח הבקרה**' < '**ביצועים ותחזוקה**' < '**אפשרויות צריכת חשמל**'.
2. בחלון '**מאפייני אפשרויות צריכת חשמל**', לחץ על הכרטיסייה '**מתקדם**'.
3. באזור '**לחצני צריכת חשמל**', בחר בהגדרה הרצויה ללחצן ההפעלה. לאחר שלחצן ההפעלה מוגדר לתפקד כלחצן השעיה, לחץ על לחצן ההפעלה כדי להעביר את המערכת למצב צריכת המתח הנמוכה ביותר (מצב השעיה). לחץ שוב על הלחצן כדי להחזיר את המערכת במהירות ממצב השעיה למצב פעולה במתח מלא. כדי לנתק לחלוטין את המתח מהמערכת, לחץ על לחצן ההפעלה ברציפות במשך 4 שניות.



זהירות: אין להשתמש בלחצן ההפעלה לכיבוי המחשב, אלא אם כן המערכת אינה מגיבה. כיבוי המחשב ללא התערבות מערכת ההפעלה עלול לגרום לנזק או לאובדן נתונים בדיסק הקשיח.

אתר האינטרנט

מהנדסי HP מבצעים בדיקות וניפוי שגיאות קפדני לכל תוכנה תוצרת HP וספקי צד שלישי, ומפתחים תוכנות תמיכה מיוחדות למערכת ההפעלה כדי להבטיח רמה מיטבית של ביצועים, תאימות ואמינות למחשבים אישיים תוצרת HP.

כשעוברים למערכת הפעלה חדשה או משופרת, חשוב להשתמש בתוכנת התמיכה שפותחה למערכת הפעלה זו. אם אתה מתכנן להריץ גרסת **חלונות** של מיקרוסופט השונה מהגרסה המותקנת במחשב, עליך להתקין דרייברים להתקנים וכלי עזר מתאימים, כדי להבטיח תמיכה ותפקוד הולם של כל התכונות הנתמכות.

חברת HP הקלה על משימות האיתור, הגישה, ההערכה וההתקנה של תוכנת התמיכה החדשה. תוכל להוריד את התוכנה באתר <http://www.hp.com/support>.

אתר האינטרנט כולל דרייברים להתקנים, כלי עזר ותצורות זיכרון הבזק עדכניים, הדרושים לצורך הרצת גרסת חלונות המתקדמת ביותר במחשב HP שברשותך.

אבני בניין ושותפים

פתרונות הניהול של HP משתלבים עם יישומי ניהול של מערכות אחרות, המבוססים על סטנדרטים מקובלים בשוק, כגון:

- Desktop Management Interface (DMI) 2.0 (ממשק לניהול שולחן העבודה 2.0)
- Wake on LAN Technology (טכנולוגיית יקיצה ברשת)
- ACPI
- SMBIOS
- תמיכה ב-Pre-boot Execution (PXE) (ביצוע קדם-אתחול)

בקרת נכסים ואבטחה

תכונות בקרת נכסים הנכללות במחשב מספקות נתוני מעקב אחר נכסים שניתן לנהלם באמצעות HP Insight Manager, HP Client Manager או יישומי ניהול מערכת אחרים. שילוב אוטומטי וחלק בין תכונות בקרת הנכסים ומוצרים אלה מאפשר לך לבחור את כלי הניהול המתאים ביותר לסביבת העבודה, ולמנוף את ההשקעה שבוצעה בכלים הקיימים.


HP מציעה גם כמה פתרונות לבקרת גישה לרכיבים ומידע חשובים במחשב. כאשר ProtectTools Embedded Security מותקן, הוא מונע גישה לא מורשית לנתונים, בודק את תקינות המערכת ומבצע אימות של משתמשי צד שלישי המנסים לבצע גישה למערכת. תכונות אבטחה הנכללות בדגמים מסוימים, כגון Smart Cover Sensor, ProtectTools (חיישן המכסה החכם) ו-Smart Cover Lock (מנעול המכסה החכם), מסייעות למנוע גישה לא מורשית לרכיבים פנימיים במחשב. באמצעות השבתת חיבורים מקביליים, טוריים או חיבורי USB, או באמצעות השבתת יכולת אתחול אמצעי אחסון שליפים, ניתן לספק הגנה לנתונים חשובים. את ההתראות על שינויי זיכרון והתראות חיישן המכסה החכם ניתן להעביר אוטומטית הלאה ליישומי ניהול מערכת במטרה למסור הודעות מוקדמות על ניסיונות חדירה למרכיבים הפנימיים של המחשב.

התכונות Smart Cover ו-Smart Cover Sensor, ProtectTools זמינות כרכיבים אופציונליים במערכות נבחרות.




- השתמש בכלי העזר הבאים כדי לנהל את הגדרות האבטחה במחשב HP :
 - באופן מקומי, באמצעות שימוש בכלי העזר Computer Setup (הגדרות המחשב). ראה מדריך לכלי העזר הגדרות המחשב (F10) שסופק יחד עם המחשב, לקבלת מידע נוסף והוראות לשימוש בכלי העזר הגדרות המחשב.
 - מרחוק, באמצעות שימוש ב-HP Client Manager או ב-System Software Manager. תוכנות אלה מאפשרות בקרה ופריסה מאובטחת ועקבית של הגדרות אבטחה מכלי עזר פשוט המופעל משורת הפקודה.

הטבלה והסעיפים הבאים מתייחסים לניהול מקומי של תכונות האבטחה של המחשב באמצעות שימוש בכלי העזר הגדרות המחשב (F10).

מבט כללי על תכונות אבטחה		
תכונה	מטרה	אופן הפעולה
Removable Media Boot Control (בקרת אתחול רכיבים נשלפים)	מניעת אתחול מכוננים שליפים. (תכונה זו זמינה בכוננים נבחרים)	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Serial, Parallel, USB, or Infrared Interface Control (בקרת ממשק טורי, ממשק מקבילי, ממשק USB או ממשק אינפרה-אדום)	מניעת העברת נתונים באמצעות ממשק טורי, מקבילי, USB או אינפרה-אדום המובנה במערכת.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Power-On Password (סיסמת הפעלה)	מניעת שימוש במחשב כל עוד לא הוזנה סיסמה. ניתן ליישם גם לגבי אתחול ראשוני ואתחול חוזר של המערכת.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Setup Password (סיסמת הגדרות)	מניעת שינוי הגדרות התצורה של המחשב (שימוש בכלי העזר הגדרות המחשב) כל עוד לא הוזנה סיסמה.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Embedded Security Device (התקן אבטחה משובץ)	מניעת גישה לא מורשית לנתונים באמצעות הצפנה והגנה על-ידי סיסמה. בדיקת תקינות המערכת ואימות משתמשי צד שלישי המנסים לבצע גישה למערכת.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
DriveLock	מניעת גישה לא מורשית לנתונים המאוחסנים בכוננים קשיחים מסוג MultiBay. תכונה זו זמינה בדגמים נבחרים בלבד.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
 למידע נוסף על הגדרות המחשב, עיין במדריך לכלי העזר הגדרות המחשב (F10). התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.		

מבט כללי על תכונות אבטחה (המשך)

תכונה	מטרה	אופן הפעולה
Smart Cover Sensor (חיישן המכסה החכם)	מציין כי מכסה המחשב או לוח הגישה הצדדי הוסרו. ניתן להגדיר את החיישן כך שיחייב להזין את סיסמת ההגדרות כדי לאתחל את המחשב לאחר הסרת המכסה או לוח הצד. ראה מדריך חומרה בתקליטור התייעוד למידע נוסף על תכונה זו. תכונה זו זמינה בדגמים נבחרים בלבד.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Master Boot Record Security (אבטחת רשומת אתחול ראשית)	אפשרות למניעת הכנסת שינויים בשגגה או בזדון ברשומת אתחול ראשית בדיסק האתחול הנוכחי, ואמצעים לאחזור רשומת האתחול הראשית התקינה האחרונה.	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Memory Change Alerts (התראות על שינויים בזיכרון).	זיהוי הוספה, העברה או הסרה של מודולי זיכרון. שליחת הודעות למשתמש ולמנהל המערכת.	לקבלת מידע אודות הפעלת Memory Change Alerts, עיין במדריך הניהול הנבון המקוון.
 למידע נוסף על הגדרות המחשב, עיין במדריך לכלי העזר הגדרות המחשב (F10). התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.		

מבט כללי על תכונות אבטחה (המשך)

תכונה	מטרה	אופן הפעולה
Ownership Tag (תגית בעלות)	הצגת מידע על בעלות, כפי שהוגדר על ידי מנהל המערכת בזמן אתחול המערכת (מוגן על ידי סיסמת הגדרות).	מתוך תפריט כלי העזר הגדרות המחשב (F10).
Cable Lock Provision (התקן מנעול כבל)	מניעת גישה לחלל הפנימי של המחשב במטרה למנוע שינויי תצורה בלתי רצויים או הסרה בלתי רצויה של רכיבים. משמש גם לצורך חיבור המחשב לעצם קבוע כדי למנוע גניבה.	התקן מנעול כבל כדי לקשור את המחשב לאובייקט קבוע.
Security Loop Provision (התקן לולאת אבטחה)	מניעת גישה לחלל הפנימי של המחשב במטרה למנוע שינויי תצורה בלתי רצויים או הסרה בלתי רצויה של רכיבים.	התקן מנעול לולאת האבטחה כדי למנוע שינויי תצורה בלתי מורשים או הסרה של רכיבים.
 למידע נוסף על הגדרות המחשב, עיין במדריך לכלי העזר הגדרות המחשב (F10). התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.		

אבטחה באמצעות סיסמה

סיסמת ההפעלה מונעת שימוש לא-חוקי במחשב בכך שהיא דורשת הזנת סיסמה לצורך גישה ליישומים או נתונים בכל פעם שמפעילים או מבצעים אתחול מחדש של המחשב האישי. סיסמת ההגדרות מיועדת במיוחד למניעת גישה לא-חוקית להגדרות מערכת, וניתן להשתמש בה כדי לדרוס את סיסמת ההפעלה. כלומר, במקרה שנדרשים להזין סיסמת הפעלה, ניתן להזין במקום זאת את סיסמת ההגדרות, וכך תתאפשר גישה למחשב האישי.

ניתן להגדיר סיסמת הגדרות לכל הרשת כדי לאפשר למנהל הרשת להתחבר לכל המחשבים ברשת לצורכי תחזוקה, מבלי שיצטרך לדעת את סיסמאות ההפעלה שלהם, גם אם הוגדרו כאלה.

קביעת סיסמת הגדרות באמצעות Computer Setup (הגדרות המחשב)

אם מותקן במחשב התקן אבטחה משובץ, עיין בפרק "אבטחה משובצת" בעמוד 30.

יצירת סיסמת הגדרות באמצעות הגדרות המחשב, מונעת ביצוע שינויים בתצורת המחשב (שימוש בכלי העזר הגדרות המחשב (F10) עד להזנת הסיסמה.

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש F10 ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש Enter כדי לעקוף את מסך הפתיחה.

אם לא הקשת F10 בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש F10 כדי לגשת לכלי העזר.



3. בחר באפשרות Security (אבטחה), ולאחר מכן בחר באפשרות Setup Password (סיסמת הגדרות) ובצע את ההוראות המוצגות על המסך.
4. לסיום, בחר File (קובץ) < Save Changes and Exit (שמירת שינויים ויציאה).

קביעת סיסמת הפעלה (Power-On) באמצעות Computer Setup (הגדרות המחשב)

קביעת סיסמת הפעלה באמצעות הגדרות המחשב מונעת גישה למחשב לאחר הפעלתו, כל עוד לא הוזנה סיסמה. לאחר הגדרת סיסמת הפעלה, הגדרות המחשב מציג את אפשרויות הסיסמה בתפריט File (אבטחה). אפשרויות הסיסמה כוללות את Password Prompt on Warm Boot (בקשה להזנת סיסמה באתחול חם). כאשר התכונה בקשת Password Prompt on Warm Boot מופעלת, יש להזין את הסיסמה בכל פעם שהמחשב מופעל מחדש.

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. בחר בתפריט **Security (אבטחה)**, לאחר מכן בחר **Power-On Password (סיסמת הפעלה)** ובצע את ההוראות המוצגות על המסך.
4. לסיום, בחר **File (קובץ)** < **Save Changes and Exit (שמירת שינויים ויציאה)**.

הזנת סיסמת הפעלה

כדי להזין סיסמת הפעלה, בצע את הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. לאחר שסמל המפתח מופיע על המסך, הקלד את הסיסמה הנוכחית ולאחר מכן הקש **Enter**.

הקפד בשעת הקלדת הסיסמה: מסיבות של אבטחה, התווים המוקלדים אינם מוצגים על המסך.



אם טעית בהקלדת הסיסמה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

הזנת סיסמת הגדרות

אם מותקן במחשב התקן אבטחה משובץ, עיין בפרק "אבטחה משובצת" בעמוד 30.

אם הוגדרה סיסמת הגדרות במחשב, תתבקש להזין סיסמה זו בכל פעם שבה תפעיל את הגדרות המחשב.

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.

2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. לאחר שסמל המפתח יופיע על המסך, הקלד את סיסמת ההגדרות והקש **Enter**.

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



אם טעית בהקלדת הסיסמה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

שינוי סיסמת הפעלה או סיסמת הגדרות

אם מותקן במחשב התקן אבטחה משובץ, עיין בפרק "אבטחה משובצת" בעמוד 30.

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'. כדי לשנות את סיסמת ההגדרות, הפעל את Computer Setup (הגדרות המחשב).
2. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית, קו נטוי (/) או תו הפרדה חלופי, סיסמה חדשה, קו נטוי (/) או תו הפרדה חלופי, והסיסמה החדשה שנית, לפי הדוגמה הבאה:
סיסמה נוכחית/סיסמה חדשה/סיסמה חדשה

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



3. הקש Enter.
- בפעם הבאה שתפעיל את המחשב, הסיסמה החדשה תיכנס לתוקף.

לקבלת מידע לגבי תווי הפרדה חלופיים, עיין בסעיף "תווי הפרדה במקלדות של שפות שונות" בעמוד 29. ניתן לשנות את סיסמת ההפעלה וסיסמת ההגדרות על-ידי שימוש באפשרויות האבטחה בהגדרות המחשב.



מחיקת סיסמת הפעלה או סיסמת הגדרות

אם מותקן במחשב התקן אבטחה משובץ, עיין בפרק "אבטחה משובצת" בעמוד 30.

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'. כדי למחוק את סיסמת ההגדרות, הפעל את הגדרות המחשב.

2. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית שלך ואחריה קו נטוי (/) או תו הפרדה חלופי לפי הדוגמה הבאה:

סיסמה נוכחית/

3. הקש Enter.



לקבלת מידע לגבי תווי הפרדה חלופיים, עיין בסעיף "תווי הפרדה במקלדות של שפות שונות" בהמשך פרק זה. ניתן לשנות את סיסמת ההפעלה וסיסמת ההגדרות על-ידי שימוש באפשרויות האבטחה בהגדרות המחשב.

תווי הפרדה במקלדות של שפות שונות

כל מקלדת מתוכננת כך שתתאים לדרישות המיוחדות של כל מדינה ומדינה. התחביר והמקשים שבהם תשתמש לשינוי או למחיקת הסיסמה, תלויים במקלדת שסופקה עם המחשב שלך.

תווי הפרדה במקלדות של שפות שונות

/	רוסית	-	יוונית	/	ערבית
-	סלובקית	.	עברית	=	בלגית
-	ספרדית	-	הונגרית	-	BHCSY*
/	שוודית/פינית	-	איטלקית	/	ברזילאית
-	שוויצרית	/	יפנית	/	סינית
/	טיוואנית	/	קוריאנית	-	צ'כית
/	תאילנדית	-	אמל"טית	-	דנית
.	טורקית	-	נורווגית	!	צרפתית
/	אנגלית (בריטניה)	-	פולנית	é	צרפתית-קנדית
/	אנגלית (ארה"ב)	-	פורטוגזית	-	גרמנית

*עבור בוסניה-הרצגובינה, קרואטיה, סלובניה ויוגוסלביה.

ביטול סיסמאות

אם שכחת את הסיסמה, לא תוכל להפעיל את המחשב. עיין במדריך לאיתור תקלות לקבלת הוראות אודות ביטול סיסמאות.
אם מותקן במחשב התקן אבטחה משובץ, עיין בפרק "אבטחה משובצת".

אבטחה משובצת (Embedded Security)

הכלי ProtectTools Embedded Security משלב הצפנה והגנה על-ידי סיסמה כדי לספק אבטחה משופרת באמצעות הצפנת קבצים/תיקיות מסוג Embedded File System (EFS) ודואר אלקטרוני מאובטח באמצעות Microsoft Outlook ו-Outlook Express. ProtectTools זמין עבור מחשבים עסקיים נבחרים כחלק מאפשרויות (CTO) Configured-To-Order. כלי זה מיועד ללקוחות HP שמייחסים חשיבות רבה לנושא אבטחת הנתונים. גישה לא מורשית לנתונים מהווה סיכון רב יותר באופן משמעותי מאובדן נתונים. ProtectTools משתמש בארבע סיסמאות:

- Setup (F10) – לכניסה לכלי העזר הגדרות המחשב (F10) והפעלה/ביטול של ProtectTools
- Take Ownership (לקיחת בעלות) – מיועדת להגדרה על-ידי מנהל המערכת ולשימוש, לצורך הענקת הרשאות למשתמשים ולהגדרת פרמטרי אבטחה
- Emergency Recovery Token (שחזור בשעת חירום) – מוגדרת על-ידי מנהל המערכת, ומאפשרת שחזור במקרה של כשל בשבב המחשב או ב-ProtectTools
- Basic User (משתמש בסיסי) – מיועדת להגדרה על-ידי משתמש הקצה ולשימוש.

אם סיסמת משתמש הקצה הולכת לאיבוד, לא ניתן לשחזר נתונים מוצפנים. לכן, השימוש ב-ProtectTools הוא הבטוח ביותר כשהנתונים הנמצאים בכונן של המשתמש מועתקים במערכת מידע של הארגון, או כשהם מגובים באופן סדיר.



ProtectTools Embedded Security הוא שבב אבטחה תואם TCPA 1.1, שיכול להיות מותקן בלוח המערכת של מחשבים עסקיים נבחרים. כל שבב ProtectTools Embedded Security הוא ייחודי וקשור למחשב ספציפי. כל שבב מבצע תהליכי אבטחה באופן בלתי תלוי ברכיבי המחשב האחרים (כגון המעבד, הזיכרון או מערכת ההפעלה).

מחשב התומך ב-ProtectTools Embedded Security משלים ומשפר את יכולות האבטחה הטבועות של חלונות 2000 או חלונות XP Professional או Home Edition של מיקרוסופט. לדוגמה, בעוד שמערכת ההפעלה יכולה להצפין קבצים ותיקיות מקומיים על בסיס EFS, ProtectTools Embedded Security מציע רובד נוסף של אבטחה על-ידי יצירת מפתחות הצפנה מתוך מפתח השורש של הפלטפורמה (המאוחסן בסיליקון). תהליך זה מוכר כ"גלישה" של מפתחות ההצפנה. ProtectTools אינו מונע גישה של הרשת למחשב ללא ProtectTools.

יכולות מרכזיות של ProtectTools Embedded Security כוללות:

- אימות פלטפורמה
- אחסון מוגן
- תקינות נתונים

זהירות: הגן על הסיסמאות. לא ניתן לגשת לנתונים מוצפנים, או לשחזרם, ללא הסיסמאות.



הגדרת סיסמאות

Setup (הגדרות)

ניתן ליצור סיסמת הגדרות, כך שהתקן האבטחה המשובצת יופעל באמצעות כלי העזר F10 setup.

1. הקש על מקש F10 ברגע שנורת המסך הופכת לירוקה.

אם לא הקשת F10 בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש F10 כדי לגשת לכלי העזר.



2. השתמש במקשי החצים למעלה או למטה כדי לבחור שפה, ולאחר מכן הקש Enter.

3. השתמש במקשי החצים שמאלה וימינה כדי לעבור לכרטיסייה Security (אבטחה), ולאחר מכן השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות Setup Password (סיסמת הגדרות). הקש Enter.

4. הקלד סיסמה ואשר אותה. הקש **F10** כדי לאשר את הסיסמה.

הקלד בזירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



5. השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות

Embedded Security Device (התקן אבטחה משובצת). הקש **Enter**.

6. אם האפשרות הנבחרת בתיבת דו-שיח זו היא **Embedded Security**

Device—Disable (התקן אבטחה משובצת – מושבת), השתמש

במקשי החצים שמאלה או ימינה כדי לשנותה ל- **Embedded Security**

Device—Enable (התקן אבטחה משובצת – מופעל). הקש **F10** כדי

לאשר את השינוי.

זהירות: אם תבחר באפשרות **Reset to Factory Settings—Reset** (איפוס

להגדרות היצרן – אפס), כל המפתחות יימחקו ולא תהיה אפשרות לשחזר

את הנתונים המוצפנים, אלא אם בוצע גיבוי של המפתחות (ראה

"Emergency Recovery Token-I Take Ownership"). בחר באפשרות **Reset**

(איפוס) רק כאשר תבקש לעשות זאת בהליך לשחזור נתונים מוצפנים (ראה

"שחזור נתונים מוצפנים" בעמוד 35).



7. השתמש במקשי החצים שמאלה או ימינה כדי לעבור לתפריט **File**

(קובץ). השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות

Save Changes and Exit (שמירת שינויים ויציאה). הקש **Enter**, ולאחר

מכן הקש **F10** כדי לאשר.

Emergency Recovery Token-I Take Ownership

סיסמת **Take Ownership** (לקיחת בעלות) דרושה לצורך הפעלה או השבתה

של פלטפורמת האבטחה, ולצורך הענקת הרשאות למשתמשים. אם התקן

האבטחה המשובצת נכשל, מנגנון השחזור ממצב חירום מאפשר

למשתמשים לקבל הרשאה ולגשת לנתונים.

1. אם אתה משתמש בחלונות **XP Professional** או **Home Edition**, לחץ

על 'התחל' < 'כל התוכניות' < **HP ProtectTools Embedded Security**

Tools (כלי אבטחה משובצת של **ProtectTools**) < **Embedded Security**

Initialization Wizard (אשף אתחול האבטחה המשובצת).

אם אתה משתמש בחלונות 2000, לחץ על 'התחל' < 'תוכניות' <

HP ProtectTools Embedded Security Tools (כלי אבטחה משובצת

של **ProtectTools**) < **Embedded Security Initialization Wizard** (אשף

אתחול האבטחה המשובצת).

2. לחץ על **Next** (הבא).

3. הקלד סיסמת **Take Ownership** ואשר אותה, ולאחר מכן לחץ על **Next**

(הבא).

הקלד בזהירות ; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



4. לחץ על Next כדי לאשר את מיקום ארכיון השחזור המשמש כברירת מחדל.

5. הקלד סיסמת Emergency Recovery Token ואשר אותה, ולאחר מכן לחץ על Next.

6. הכנס תקליטון שבו תאחסן את מפתח Emergency Recovery Token. לחץ על Browse (עיון) ובחר את התקליטון.

זהירות: מפתח Emergency Recovery Token משמש לשחזור נתונים מוצפנים במקרה של כשל במחשב או בשבב האבטחה המשובצת. **לא ניתן לשחזר את הנתונים ללא המפתח.** (עדיין אין אפשרות גישה לנתונים ללא סיסמת Basic User (משתמש בסיסי)). שמור תקליטון זה במקום בטוח.



7. לחץ על Save (שמור) כדי לאשר את המיקום ושם הקובץ המוגדר כברירת מחדל, ולאחר מכן לחץ על Next.

8. לחץ על Next כדי לאשר את ההגדרות לפני אתחול פלטפורמת האבטחה.

ייתכן שתוצג הודעה שתציין כי תכונות האבטחה המשובצת אינן מאותחלות. אל תלחץ על ההודעה, נושא זה יטופל בהמשך, וההודעה תיסגר לאחר שניות אחדות.



9. לחץ על Next כדי לעקוף מדיניות מקומית של קביעת תצורה.

10. ודא שתיבת הסימון Start Embedded Security User Initialization Wizard (אשף אתחול משתמשי אבטחה משובצת) נבחרה, ולאחר מכן לחץ על Finish (סיום).

User Initialization Wizard (אשף אתחול המשתמש) מופעל כעת באופן אוטומטי.

Basic User (משתמש בסיסי)

במהלך אתחול המשתמש, נוצרת סיסמת Basic User (משתמש בסיסי).
סיסמה זו דרושה להזנת נתונים מוצפנים ולקבלת גישה אליהם.

זהירות: הגן על סיסמת Basic User. לא ניתן לגשת לנתונים מוצפנים, או לשחזרם, ללא סיסמה זו.



1. אם אשף אתחול המשתמש לא נפתח:

אם אתה משתמש בחלונות XP Professional או ב- Home Edition, לחץ על 'התחל' < 'כל התוכניות' < HP ProtectTools Embedded Security Tools (כלי אבטחה משובצת של ProtectTools) < User Initialization Wizard (אשף אתחול המשתמש).

אם אתה משתמש בחלונות 2000, לחץ על 'התחל' < 'תוכניות' < HP ProtectTools Embedded Security Tools (כלי אבטחה משובצת של ProtectTools) < User Initialization Wizard (אשף אתחול המשתמש).

2. לחץ על Next (הבא).

3. הקלד סיסמת Basic User Key (מפתח משתמש בסיסי) ואשר אותה, ולאחר מכן לחץ על Next (הבא).

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



4. לחץ על Next (הבא) כדי לאשר את ההגדרות.

5. בחר את תכונות האבטחה המתאימות ולחץ על Next (הבא).

6. לחץ על לקוח הדואר האלקטרוני כדי לבחור בו, ולאחר מכן לחץ על Next (הבא).

7. לחץ על Next כדי להחיל את Encryption Certificate (אישור ההצפנה).

8. לחץ על Next (הבא) כדי לאשר את ההגדרות.

9. לחץ על Finish (סיום).

10. הפעל מחדש את המחשב.

שחזור נתונים מוצפנים

כדי לשחזר נתונים לאחר החלפת שבב ProtectTools, דרושים לך הפריטים הבאים:

- SPEmRecToken.xml - מפתח Emergency Recovery Token (שחזור ממצב חירום)
- SPEmRecArchive.xml – תיקייה מוסתרת, מיקום ברירת המחדל:
C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- סיסמאות ProtectTools
 - ☐ Setup (הגדרות)
 - ☐ Take Ownership (לקיחת בעלות)
 - ☐ Emergency Recovery Token (Token של שחזור ממצב חירום)
 - ☐ Basic User (משתמש בסיסי)

1. הפעל מחדש את המחשב.

2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. הקלד את סיסמת ההגדרות, ולאחר מכן הקש **Enter**.

4. השתמש במקשי החצים למעלה או למטה כדי לבחור שפה, ולאחר מכן הקש **Enter**.

5. השתמש במקשי החצים שמאלה וימינה כדי לעבור לכרטיסייה **Security** (אבטחה), ולאחר מכן השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Embedded Security Device** (התקן אבטחה משובצת). הקש **Enter**.

6. במקרה שאפשרות אחת בלבד, **Embedded Security Device—Disable**, (התקן אבטחה משובצת – השבת), זמינה:

א. השתמש במקשי החצים שמאלה או ימינה כדי לשנותה לאפשרות **Embedded Security Device—Enable** (התקן אבטחה משובצת – הפעל). הקש **F10** כדי לאשר את השינוי.

ב. השתמש במקשי החצים שמאלה או ימינה כדי לעבור לתפריט **File** (קובץ). השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Save Changes and Exit** (שמירת שינויים ויציאה). הקש **Enter**, ולאחר מכן הקש **F10** כדי לאשר.

ג. עבור לשלב 1.

אם שתי האפשרויות זמינות, עבור לשלב 7.

7. השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Reset to Factory Settings** (איפוס להגדרות היצרן – אל תאפס). הקש פעם אחת על מקש החץ השמאלי או הימני. תוצג הודעה: ביצוע פעולה זו יגרום לאיפוס התקן האבטחה המשובצת להגדרות היצרן אם ההגדרות נשמרות ביציאה. הקש על מקש כלשהו כדי להמשיך.

הקש **Enter**.

8. האפשרות תשתנה ל-**Reset—Reset to Factory Settings** (איפוס להגדרות היצרן – אפס). הקש **F10** כדי לאשר את השינוי.

9. השתמש במקשי החצים שמאלה או ימינה כדי לעבור לתפריט **File** (קובץ). השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Save Changes and Exit** (שמירת שינויים ויציאה). הקש **Enter**, ולאחר מכן הקש **F10** כדי לאשר.

10. הפעל מחדש את המחשב.

11. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



12. הקלד את סיסמת ההגדרות, ולאחר מכן הקש **Enter**.

13. השתמש במקשי החצים למעלה או למטה כדי לבחור שפה, ולאחר מכן הקש **Enter**.

14. השתמש במקשי החצים שמאלה וימינה כדי לעבור לכרטיסייה **Security** (אבטחה), ולאחר מכן השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Embedded Security Device** (התקן אבטחה משובצת). הקש **Enter**.

15. אם האפשרות הנבחרת בתיבת דו-שיח זו היא **Embedded Security Device—Disable** (התקן אבטחה משובצת – מושבת), השתמש במקשי החצים שמאלה או ימינה כדי לשנותה ל-**Embedded Security Device—Enable** (התקן אבטחה משובצת – מופעל). הקש **F10**.

16. השתמש במקשי החצים שמאלה או ימינה כדי לעבור לתפריט **File** (קובץ). השתמש במקשי החצים למעלה או למטה כדי לעבור לאפשרות **Save Changes and Exit** (שמירת שינויים ויציאה). הקש **Enter**, ולאחר מכן הקש **F10** כדי לאשר.

17. לאחר שמערכת ההפעלה חלונית נפתחת :

אם אתה משתמש בחלונות XP Professional או ב-Home Edition, לחץ על 'התחל' < 'כל התוכניות' < **HP ProtectTools Embedded Security Tools** (כלי אבטחה משובצת של ProtectTools) < **Embedded Security Initialization Wizard** (אשף אתחול האבטחה המשובצת).

אם אתה משתמש בחלונות 2000, לחץ על 'התחל' < 'תוכניות' < **HP ProtectTools Embedded Security Tools** (כלי אבטחה משובצת של ProtectTools) < **Embedded Security Initialization Wizard** (אשף אתחול האבטחה המשובצת).

18. לחץ על **Next** (הבא).

19. הקלד סיסמת **Take Ownership** ואשר אותה. לחץ על **Next** (הבא).

הקלד בזהירות ; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.



20. ודא שהאפשרות **Create a new recovery archive** (צור ארכיון שחזור חדש) מסומנת. תחת **Recovery archive location** (מיקום ארכיון שחזור), לחץ על **Browse** (עיון).

21. אל תאשר את שם הקובץ המוגדר כברירת מחדל. הקלד שם קובץ חדש כדי למנוע את החלפת שם הקובץ המקורי.

22. לחץ על **Save** (שמור), ולאחר מכן לחץ על **Next** (הבא).

23. הקלד סיסמת **Emergency Recovery Token** ואשר אותה, ולאחר מכן לחץ על **Next**.

24. הכנס תקליטון שבו תאחסן את מפתח **Emergency Recovery Token**. לחץ על **Browse** (עיון) ובחר את התקליטון.

25. אל תאשר את שם המפתח המוגדר כברירת מחדל. הקלד שם מפתח חדש כדי למנוע את החלפת שם המפתח המקורי.

26. לחץ על **Save** (שמור), ולאחר מכן לחץ על **Next** (הבא).

27. לחץ על **Next** כדי לאשר את ההגדרות לפני אתחול פלטפורמת האבטחה.

ייתכן שתוצג הודעה, שתציין כי לא ניתן לטעון את מפתח המשתמש הבסיסי. אל תלחץ על ההודעה, נושא זה יטופל בהמשך, וההודעה תיסגר לאחר שניות אחדות.



28. לחץ על **Next** כדי לעקוף מדיניות מקומית של קביעת תצורה.

29. לחץ על תיבת הסימון **Start Embedded Security User Initialization Wizard** (הפעל את אשף אתחול משתמשי אבטחה משובצת) כדי לנקותה. לחץ על **Finish** (סיום).

30. לחץ באמצעות לחצן העכבר הימני על סמל ProtectTools בסרגל הכלים, ולחץ על האפשרות **Initialize Embedded Security restoration** (אתחול שחזור אבטחה משובצת).
- פעולה זו תפעיל את HP ProtectTools Embedded Security Initialization Wizard (אשף אתחול האבטחה המשובצת של HP ProtectTools).
31. לחץ על **Next** (הבא).
32. הכנס את התקליטון שבו שמרת את מפתח Emergency Recovery Token המקורי. לחץ על **Browse** (עיון), ולאחר מכן אתר את ה-Token ולחץ עליו פעמיים כדי להזין את השם בשדה. ברירת המחדל היא A:\SPEmRecToken.xml.
33. הקלד את סיסמת Token המקורית, ולחץ על **Next** (הבא).
34. לחץ על **Browse** (עיון), ולאחר מכן אתר את ארכיון השחזור המקומי ולחץ עליו פעמיים כדי להזין את השם בשדה. ברירת המחדל היא:
C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. לחץ על **Next** (הבא).
36. לחץ על המחשב שברצונך לשחזר ולחץ על **Next** (הבא).
37. לחץ על **Next** (הבא) כדי לאשר את ההגדרות.
38. אם האשף מודיע כי פלטפורמת האבטחה לא שוחזרה, עבור לשלב 39. אם האשף מודיע שהשחזור נכשל, חזור לשלב 10. בדוק בזהירות את הסיסמאות, את מיקום ה-Token ואת שמו, וכן את מיקום הארכיון ואת שמו.
39. לחץ על **Finish** (סיום).
40. אם אתה משתמש בחלונות XP Professional או ב-Home Edition, לחץ על '**התחל**' < '**כל התוכניות**' < **HP ProtectTools Embedded Security Tools** (כלי אבטחה משובצת של ProtectTools) < **User Initialization Wizard** (אשף אתחול המשתמש).
- אם אתה משתמש בחלונות 2000, לחץ על '**התחל**' < '**תוכניות**' < **HP ProtectTools Embedded Security Tools** (כלי אבטחה משובצת של ProtectTools) < **User Initialization Wizard** (אשף אתחול המשתמש).
41. לחץ על **Next** (הבא).
42. לחץ על **Recover your basic user key** (שחזר את מפתח המשתמש הבסיסי) ולאחר מכן לחץ על **Next** (הבא).
43. בחר משתמש, הקלד סיסמת Basic User Key (מפתח משתמש בסיסי) מקורית עבור אותו משתמש, ולאחר מכן לחץ על **Next** (הבא).

44. לחץ על Next (הבא) כדי לאשר את ההגדרות ואת מיקום נתוני השחזור המוגדר כברירת מחדל.

בשלב 45 עד 49 מתבצעת התקנה מחדש של תצורת המשתמש הבסיסי המקורית.



45. בחר את תכונות האבטחה המתאימות ולחץ על Next (הבא).

46. לחץ על לקוח הדואר האלקטרוני כדי לבחור בו, ולאחר מכן לחץ על Next (הבא).

47. לחץ על Encryption Certificate (אישור הצפנה) ולאחר מכן לחץ על Next (הבא) כדי להחיל אפשרות זו.

48. לחץ על Next (הבא) כדי לאשר את ההגדרות.

49. לחץ על Finish (סיום).

50. הפעל מחדש את המחשב.

זהירות: הגן על סיסמת Basic User. לא ניתן לגשת לנתונים מוצפנים, או לשחזרם, ללא סיסמה זו.



DriveLock

DriveLock היא תכונת אבטחה מקובלת בתעשייה המונעת גישה לא-חוקית לנתונים בדיסקים קשיחים מסוג MultiBay DriveLock. מיושם כהרחבה להגדרות המחשב. אפשרות זו זמינה רק בעת זיהוי דיסקים קשיחים התומכים ב-DriveLock.

DriveLock מיועד ללקוחות HP שמייחסים חשיבות רבה לנושא אבטחת הנתונים. ללקוחות כאלה, עלות של דיסק קשיח היא זניחה בהשוואה לנזק העלול לנבוע מגישה לא-חוקית לתוכן הדיסק הקשיח. כדי לאזן בין רמה גבוהה זו של אבטחה לבין הצורך השכיח לקבלת סיסמה שנשכחה, DriveLock מפעיל סכימת אבטחה בעלת שתי סיסמאות. סיסמה אחת מיועדת לשמש את מנהל המערכת, ואילו הסיסמה השנייה משמשת בדרך כלל את משתמש הקצה. אין שום דרך לשחרור הכוון אם שתי הסיסמאות אובדות. לכן, השימוש ב-DriveLock הוא הבטוח ביותר כשנתונים הנמצאים בדיסק הקשיח מועתקים במערכת מידע שיתופית, או כשהם מגובים באופן סדיר.

במקרה ששתי סיסמאות DriveLock נשכחו, לא ניתן יהיה להשתמש בדיסק הקשיח. לגבי משתמשים שאינם מתאימים לפרופיל הלקוחות המוגדר, הדבר עלול לגרום סיכון חמור. לגבי משתמשים המתאימים לפרופיל הלקוחות, הסיכון הוא סביר בהתחשב באופי הנתונים השמורים בדיסק הקשיח.

שימוש ב-DriveLock

האפשרות DriveLock מופיעה בתפריט אבטחה שבהגדרות המחשב. למשתמש מוצגת אפשרות להגדיר סיסמת מנהל מערכת או להפעיל את DriveLock. יש להזין את סיסמת המשתמש כדי להפעיל את DriveLock. מכיוון שהגדרת התצורה הראשונית של DriveLock מבוצעת בדרך כלל על ידי מנהל המערכת, יש להגדיר תחילה סיסמת מנהל מערכת. HP מעודדת את מנהלי המערכת להגדיר סיסמת מנהל מערכת גם כשבכוונתם להפעיל את DriveLock, וגם כשבכוונתם להשבית את פעולתו. הדבר יספק למנהל המערכת יכולת לשנות את הגדרות DriveLock במקרה שהכוון יינעל בעתיד. לאחר הגדרת סיסמת מנהל מערכת יכול מנהל המערכת להחליט אם להפעיל את DriveLock או להמשיך להשבית אותו.

אם נמצא דיסק קשיח נעול, תדרוש הבדיקה העצמית של המחשב סיסמה כדי לשחרר את ההתקן. אם הוגדרה סיסמת הפעלה, והיא תואמת את סיסמת המשתמש של ההתקן, הבדיקה העצמית של המחשב לא תדרוש מהמשתמש להזין מחדש את הסיסמה. אחרת, יידרש המשתמש להזין סיסמת DriveLock. גם סיסמת מנהל מערכת וגם סיסמת המשתמש מתאימות למקרה זה. למשתמשים יינתנו שני ניסיונות להזין את הסיסמה הנכונה. אם שני הניסיונות יכשלו, הבדיקה העצמית תמשיך להתבצע, אך הנתונים שבכוון לא יהיו זמינים.

יישומי DriveLock

השימוש המעשי ביותר בתכונת האבטחה של DriveLock הוא בסביבה שיתופית, שבה מנהל המערכת מספק למשתמשים בדיסקים קשיחים של MultiBay לשימוש במחשבים מסוימים. מנהל המערכת אחראי להגדיר תצורת דיסק קשיח מסוג MultiBay, והדבר מחייב בין השאר להגדיר סיסמת מנהל מערכת של DriveLock. במקרה שהמשתמש שוכח את סיסמת המשתמש או שהציוד מועבר לעובד אחר, ניתן לעשות שימוש בסיסמת מנהל מערכת כדי להגדיר מחדש את סיסמת המשתמש ולזכות בגישה לדיסק הקשיח.


HP ממליצה כי מנהל מערכת שיתופית שיבחר להפעיל את DriveLock, יגדיר גם מדיניות שיתופית לצורך הגדרה ותחזוקה של סיסמאות מנהלי מערכת. הדבר חייב להתבצע כדי למנוע מצב שבו העובד יפעיל בשגגה או בזדון את שתי סיסמאות DriveLock לפני פרישתו מהחברה. בתרחיש כזה לא ניתן יהיה להשתמש בכוון הקשיח, ויהיה צורך להחליפו. באופן דומה, אם לא

תוגדר סיסמת מנהל מערכת, יוכלו מנהלי המערכת לגלות אם הדיסק הקשיח נעול וכי אין ביכולתם לבצע בדיקות שגרתיות לתוכנה לא-חוקית, פונקציות בקרת נכסים נוספות ופעולות תמיכה.

למשתמשים בעלי דרישות אבטחה חמורות פחות, HP אינה ממליצה להפעיל את DriveLock. משתמשים הנמצאים בקטגוריה זו כוללים משתמשים אישיים או משתמשים שאינם מחזיקים מידע יומיומי רגיש בדיסקים הקשיחים שלהם. למשתמשים אלה, קריסה אפשרית של הדיסק הקשיח כתוצאה משכיחת שתי הסיסמאות חשובה הרבה יותר מערך הנתונים ש-DriveLock נועד לאבטח. ניתן להגביל את הגישה להגדרות מערכת ול-DriveLock באמצעות סיסמת הגדרות. הגדרת סיסמת הגדרות מבלי למוסרה למשתמשי הקצה מאפשרת למנהלי המערכת להגביל את יכולת המשתמשים להפעיל את DriveLock.

Smart Cover Sensor (חיישן המכסה החכם)

חיישן המכסה החכם הקיים בדגמים מסוימים הוא צירוף של טכנולוגיות חומרה ותוכנה, המאפשר להציג התרעות במקרה של הסרת מכסה המחשב או לוח הצד. קיימות שלוש רמות הגנה, כמתואר בטבלה הבאה.

רמות הגנה של חיישן המכסה החכם		
רמה	הגדרה	תיאור
רמה 0	Disabled (מושבת)	חיישן המכסה החכם מושבת (ברירת מחדל).
רמה 1	Notify User (הודעה למשתמש)	כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שמכסה המחשב או לוח הצד הוסרו.
רמה 2	Setup Password (סיסמת הגדרות)	כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שמכסה המחשב או לוח הצד הוסרו. יש להזין סיסמת הגדרות כדי להמשיך.
 הגדרות אלה ניתנות לשינוי באמצעות הגדרות המחשב. למידע נוסף על הגדרות המחשב, עיין במדריך לכלי העזר הגדרות המחשב (F10).		

הגדרת רמת ההגנה של חיישן המכסה החכם

כדי להגדיר את רמת האבטחה של חיישן המכסה החכם, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. בחר באפשרות **Security** (אבטחה), לאחר מכן בחר באפשרות **Smart Cover** (מכסה חכם) ובצע את ההוראות המוצגות על המסך.
4. לסיום, בחר **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

Smart Cover Lock (מנעול המכסה החכם)

Smart Cover Lock הוא מנעול מכסה הנשלט על-ידי תוכנה, הנכלל בדגמים נבחרים של HP. נעילה זו מונעת גישה לא חוקית לרכיבים הפנימיים של המחשב. המחשבים מסופקים כאשר מנעול המכסה החכם נמצא במצב לא נעול.

זהירות: כדי להגיע לרמת האבטחה המרבית של מנעול המכסה החכם, הקפד להגדיר סיסמת הגדרות. סיסמת ההגדרות מונעת גישה בלתי מורשית לכלי העזר הגדרות המחשב.



מנעול המכסה החכם זמין כרכיב אופציונלי בדגמים נבחרים.



נעילת מנעול המכסה החכם

כדי להפעיל ולנעול את מנעול המכסה החכם, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.



אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.

3. בחר באפשרויות **Security** (אבטחה), ולאחר מכן בחר באפשרויות **Smart Cover** (מכסה חכם) ובחר באפשרויות **Locked** (נעול).
4. לסיום, בחר **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

שחרור מנעול המכסה החכם

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.



אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.

3. בחר **Security** (אבטחה) < **Smart Cover** (מכסה חכם) < **Unlocked** (שחרור נעילה).
4. לסיום, בחר **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

שימוש במפתח אל-כשל (FailSafe) של המכסה החכם

אם הפעלת את מנעול המכסה החכם, ואינך יכול להזין סיסמה כדי להשבית את המנעול, תצטרך מפתח אל-כשל למכסה החכם כדי לפתוח את מכסה המחשב. תזדקק למפתח בכל אחד מהמקרים הבאים:

- הפסקת חשמל
- כשל באתחול
- כשל של אחד מרכיבי המחשב האישי (כגון מעבד או ספק מתח)
- סיסמה שנשכחה

זהירות: מפתח אל-כשל של המכסה החכם הוא כלי ייחודי המסופק על ידי HP. הזמן מראש מפתח זה לפני שתזדקק לו בפועל אצל ספק או מוקד שירות מורשה.



כדי לקבל את מפתח האל-כשל (FailSafe), בצע אחת מהפעולות הבאות:

■ פנה לסוכן מכירות או לספק שירות מורשים של HP.

■ התקשר למספר הרשום בכתב האחריות.

למידע נוסף לגבי השימוש במפתח אל-כשל של המכסה החכם, עיין במדריך חומרה.

Master Boot Record Security (אבטחת רשומת אתחול ראשית)

רשומת האתחול הראשית (Master Boot Record, MBR) כוללת מידע הנדרש לביצוע אתחול מוצלח מהדיסק וגישה לנתונים השמורים בדיסק. אבטחת רשומת האתחול הראשית יכולה למנוע ביצוע שינויים בשגגה או בזדון ברשומת האתחול הראשית, כגון שינויים הנגרמים עקב וירוסים או שימוש לא נכון בעזרי דיסק מסוימים. האבטחה מאפשרת גם לשחזר את רשומת האתחול הראשית התקינה האחרונה, במקרה שהמערכת תזוהה כי בוצעו בה שינויים בעת הפעלה מחדש של המחשב.

כדי להפעיל אבטחת רשומת אתחול ראשית, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על 'התחל' < 'כיבוי' < 'הפעל את המחשב מחדש'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. בחר **Security** (אבטחה) < **Master Boot Record Security** (אבטחת רשומת אתחול ראשית) < **Enabled** (מופעל).
4. בחר **Security** (אבטחה) < **Save Master Boot Record** (שמור רשומת אתחול ראשית).
5. לסיום, בחר **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

כאשר אבטחת רשומת האתחול הראשית מופעלת, BIOS מונע ביצוע שינויים ברשומת האתחול הראשית של דיסק האתחול הנוכחי, כל זמן שהמחשב נמצא ב-MS-DOS או במצב בטוח בסביבת חלונות.



רוב מערכות ההפעלה שולטות בגישה לרשומת האתחול הראשית של דיסק האתחול הנוכחי; ל-BIOS אין אפשרות למנוע שינויים המתבצעים בזמן פעולת מערכת ההפעלה.

בכל פעם שמדליקים את המחשב או מפעילים אותו מחדש, ה-BIOS משווה את רשומת האתחול הראשית של דיסק האתחול הנוכחי לרשומת האתחול הראשית שנשמרה קודם. אם מתגלים שינויים ואם דיסק האתחול הנוכחי הוא אותו דיסק שבו נשמרה רשומת האתחול הראשית הקודמת, מוצגת ההודעה הבאה:

1999 - Master Boot Record has changed - 1999
רשומת האתחול הראשית השתנתה.

הקש על מקש כלשהו כדי להיכנס להגדרות לצורך הגדרה מחדש של תצורת אבטחת רשומת האתחול הראשית.

עם הכניסה ל-Computer Setup (הגדרות המחשב), בצע את הצעדים הבאים :

■ שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי ;

■ אחזר את רשומת האתחול הראשית שנשמרה קודם לכן ; או

■ השבת את תכונת אבטחת רשומת האתחול הראשית.

עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

אם זוהו שינויים ואם דיסק האתחול הנוכחי איננו הדיסק שבו נשמרה

רשומת האתחול הראשית הקודמת, תוצג ההודעה הבאה :

Master Boot Record Hard Drive has changed-2000 – רשומת

האתחול הראשית בדיסק הקשיח השתנתה).

הקש על מקש כלשהו כדי להיכנס להגדרות להגדיר את תצורת אבטחת

רשומת האתחול הראשית.

עם הכניסה להגדרות המחשב, בצע את הצעדים הבאים :

■ שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי ; או

■ השבת את תכונת אבטחת רשומת האתחול הראשית.

עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

במקרה הבלתי סביר שרשומת האתחול הראשית שנשמרה קודם לכן נפגמה,

תוצג ההודעה הבאה :

Master Boot Record has been lost - 1998 - רשומת האתחול

הראשית אבדה).

הקש על מקש כלשהו כדי להיכנס להגדרות להגדיר את תצורת אבטחת

רשומת האתחול הראשית.

עם הכניסה להגדרות המחשב, בצע את הצעדים הבאים :

■ שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי ; או

■ השבת את תכונת אבטחת רשומת האתחול הראשית.

עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

לפני הגדרת מחיצות או ביצוע פורמט של דיסק האתחול הנוכחי

ודא שאבטחת רשומת האתחול הראשית מושבתת לפני ביצוע שינויים במחיצות או פירמוט דיסק האתחול הנוכחי. עזרי דיסק מסוימים, כגון FORMAT ו-FDISK, מנסים לעדכן את רשומת האתחול הראשית. אם אבטחת רשומת האתחול הראשית מופעלת בשעת ביצוע שינויים במחיצות או פורמט לדיסק, ייתכן שתתקבל הודעת שגיאה מכלי העזר של הדיסק, או אזהרה מאבטחת רשומת האתחול הראשית בפעם הבאה שהמחשב יודלק או יופעל מחדש. כדי להשבית את אבטחת רשומת האתחול הראשית, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. אם אתה עובד בחלונות, לחץ על '**התחל**' < '**כיבוי**' < '**הפעל את המחשב מחדש**'.
2. הקש על מקש **F10** ברגע שנורת המסך הופכת לירוקה. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך לכבות את המחשב, להדליק אותו שוב, ולהקיש שוב על מקש **F10** כדי לגשת לכלי העזר.



3. בחר **Security** (אבטחה) < **Master Boot Record Security** (אבטחת רשומת אתחול ראשית) < **Disabled** (מושבת).
4. לסיום, בחר **File** (קובץ) < **Save Changes and Exit** (שמירת שינויים ויציאה).

Cable Lock Provision (התקן מנעול כבל)

הלוח האחורי של המחשב כולל מנעול כבל, כך שניתן לאבטח את המחשב פיזית למשטח העבודה.
לקבלת הוראות מלוות באיורים, אנא עיין במדריך חומרה שבתקליטור התייעוד.

טכנולוגיה לזיהוי טביעות אצבעות

הטכנולוגיה לזיהוי טביעות האצבעות של HP מעלה את רמת האבטחה של הרשת באמצעות ביטול הצורך בהזנת סיסמת משתמש, מפשטת את תהליך ההתחברות לרשת ומצמצמת עלויות ניהול של רשתות שיתופיות. זוהי טכנולוגיה שמחירה סבירים, ואינה מיועדת אך ורק לחברות היי-טק או ארגונים הדורשים רמת אבטחה גבוהה.

התמיכה בטכנולוגית זיהוי טביעות האצבעות משתנה מדגם לדגם.



לקבלת מידע נוסף, בקר בכתובת:

<http://h18000.www1.hp.com/solutions/security>

הודעות כשל והתאוששות

תכונות דיווח על תקלות והתאוששות משלבות טכנולוגיה חדשנית של חומרה ותוכנה כדי למנוע אובדן של נתונים קריטיים וכדי להקטין למינימום הפסקות עבודה בלתי מתוכננות.

במקרה של כשל, המחשב מציג הודעת התראה מקומית, הכוללת את תיאור הכשל ואת הפעולות המומלצות לתיקונו. לאחר מכן ניתן לראות את מצבה השוטף של המערכת באמצעות סוכן הניהול של HP. אם המחשב מחובר לרשת המנוהלת על ידי HP Insight Manager, HP Client Manager או יישומי ניהול מערכת אחרים, המחשב שולח גם הודעת כשל ליישום ניהול הרשת.

Drive Protection System (מערכת להגנה על כוננים)

Drive Protection System (DPS) (מערכת להגנה על כוננים) הוא כלי אבחון הנכלל בדיסקים קשיחים המותקנים במחשבים נבחרים של HP. DPS מיועד לסייע באבחון בעיות שעלולות להתעורר כתוצאה מהחלפה מיותרת של הדיסק הקשיח.

בתהליך ההרכבה של מחשבי HP, כל דיסק קשיח המותקן בהם עובר בדיקה באמצעות DPS, ורשומה קבועה עם פרטי המפתח נכתבת בכונן. בכל פעם שמריצים את DPS, תוצאות הבדיקה מאוחסנות בדיסק הקשיח. ספק השירות יכול להיעזר במידע זה לצורך אבחון הנסיבות שגרמו לך להריץ את תוכנת DPS. לקבלת הוראות שימוש ב-DPS, עיין במדריך לאיתור תקלות.

עמידה בנחשולי מתח

עמידה בנחשולי מתח מאפשרת אמינות גבוהה יותר במקרים שבהם המחשב האישי נפגע מנחשול מתח בלתי צפוי. אספקת מתח מסוג זה מתוכננת לעמוד בפני נחשולי מתח של עד 2000V ללא קריסת מערכת או אובדן מידע כלשהו.

חיישן תרמי

חיישן תרמי הוא תכונה המשלבת חומרה ותוכנה, העוקבת אחר הטמפרטורה הפנימית של המחשב. תכונה זו מציגה הודעת אזהרה אם חלה חריגה מהתחום הנורמלי, ובכך ניתן לך די זמן לנקוט פעולה לפני שייגרם נזק לרכיבים פנימיים ולפני שיאבדו נתונים.

אינדקס

א

אבטחה

41 עד 39, Drivelock

41 עד 39, MultiBay

39 עד 30, ProtectTools

סיסמה, 25

רשומת אתחול ראשית, 45 עד 46

תכונות, טבלה, 22

אבטחה משובצת של ProtectTools, 30 עד 39

מפתח שחזור ממצב חירום, 32

שחזור ממצב חירום, 35 עד 39

אבטחת MultiBay, 39 עד 41

אבטחת מנעול מכסה, זהירות, 42

אבטחת רשומת אתחול ראשית, 45 עד 46

אמצעי זהירות

אתרי אינטרנט

6, ActiveUpdate

5, Altiris PC Transplant Pro

5, Altiris

4, HP Client Manager

8, HPQFlash

6, Proactive Change Notification

ROM Flash (זיכרון הבזק ROM

מרחוק), 7

ROM Flash (זיכרון הבזק ROM), 7

זיהוי טביעות אצבעות, טכנולוגיה, 48

טכנולוגיית זיהוי טביעות אצבעות, 48

מנהל תוכנת מערכת (SSM), 6

פריסת מחשב אישי, 2

שכפול הגדרות, 12

תמונות ROMPaq, 7

תמיכה בתוכנה, 20

ב

ביטול סיסמה, 30

בקרת נכסים, 21

ג

גישה למחשב, שליטה, 21

ד

דיווח על כשל, 48

דיווח על שינוי, 6

דיסק, שכפול, 2

דיסקים קשיחים, כלי אבחון, 48

ה

הגדרות

הגדרה, 25

ראשוניות, 2

שכפול, 10

הגדרות מרחוק, 3

הגדרות, הגדרה, 21

הגדרת לחצן הפעלה, 19

הגנה על דיסק קשיח, 48

הגנה על זיכרון ROM, זהירות, 7

הודעה על שינויים, 6

הזמנת מפתח אל-כשל, 44

הזנה

סיסמת הגדרות, 27

סיסמת הפעלה, 26

הפעלה, 26

התאוששות, 2

Remote ROM Flash (זיכרון הבזק ROM

מרחוק), 7

התקנת מערכת מרחוק, 3

התאמה אישית של תוכנה, 2

התקן USB flash media, בר-אתחול, 13 עד 18

התקן בר-אתחול

DiskOnKey, 13 עד 18

HP Drive Key, 13 עד 18

התקן USB flash media, 13 עד 18

יצירה, 12 עד 18

תקליטון, 12

התקן מנעול כבל, 47

התקנת מערכת מרחוק, גישה, 3

ז

זיכרון מערכת לא תקף, 8

ח

- חיישן מכסה חכם (Smart Cover Sensor), 41
- הגדרה, 42
- רמות הגנה, 41
- חיישן תרמי, 49
- חלוקת הדיסק למחיצות, מידע חשוב, 47

ט

- טכנולוגיית זיהוי טביעות אצבעות, 48
- טמפרטורה פנימית של המחשב, 49
- טמפרטורה פנימית של המחשב, 49

ה

- כונן, הגנה, 48
- כלי אבחון לדיסקים קשיחים, 48
- כלי העזר Computer Setup (הגדרות מחשב) (F10)
- כלי פריסה, תוכנה, 2
- כלי שכפול, תוכנה, 2
- כתובת URL (אתרי אינטרנט). ראה אתרי אינטרנט.
- כתובת אינטרנט, ראה אתרי אינטרנט

ל

- לחצן הפעלה
- דו-מצבי, 19
- קביעת תצורה, 19
- לחצן הפעלה דו-מצבי, 19

מ

- מחיקת סיסמה, 29
- מכסה חכם, מנעול, 42
- מנהל תוכנת המערכת, 6
- עדכון מחשבים מרובים, 6
- מנהל תוכנת מערכת (SSM), 6
- אבטחת מנעול מכסה חכם, 42
- הגנה על זיכרון ROM, 7
- מפתח אל-כשל, 44
- מנעול מכסה חכם, 42 עד 44
- מנעול מכסה חכם, 42 עד 44
- נעילה, 43
- שחרור נעילה, 43
- מפתח אל-כשל
- הזמנה, 44
- זהירות, 44
- מפתח אל-כשל למכסה חכם, הזמנה, 44

נ

- נורות מקלדת, ROM, טבלה, 9
- נחשולי מתח, עמידה, 49
- נעילת מנעול מכסה חכם, 43

O

סיסמאות

- Basic User (משתמש בסיסי), 34
- PXE (Preboot Execution Environment), 3
- Setup (הגדרות), 31
- Take Ownership (לקיחת בעלות), 32
- Token של שחזור ממצב חירום, 32

סיסמה

- ביטול, 30
- מחיקה, 29
- שינוי, 28
- סיסמת הגדרות
- הזנה, 27
- מחיקה, 29
- שינוי, 28

ע

- עמידה בנחשולי מתח, 49

פ

- פירמוט תקליטון, מידע חשוב, 47

ש

- שדרוג זיכרון ROM, 7
- שחזור ממצב חירום, ProtectTools, 35 עד 39
- שחזור מערכת, 8
- שחזור מערכת, 8
- שחזור נתונים מוצפנים, 35 עד 39
- שחזור, תוכנה, 2
- שחרור נעילת מנעול מכסה חכם, 43
- שינוי מערכות הפעלה, מידע חשוב, 20
- שינוי מערכות הפעלה, מידע חשוב, 20
- שינוי סיסמה, 28
- שליטה על הגישה למחשב, 21
- שפות שונות, תווי הפרדה של המקלדת, 29

P

- 6, (Proactive Change Notification) PCN
- Power-On Password (סיסמת הפעלה)
- 26, הזנה
- מחיקה, 29
- שינוי, 28
- 3, (PXE) Preboot Execution Environment
- 6, (PCN) Proactive Change Notification
- ProtectTools, 31 עד 34
- אבטחה, 25
- הגדרות, 25, 27
- ProtectTools, אבטחה משובצת, 30 עד 39

R

- 7, Remote ROM Flash (זיכרון הבזק ROM מרחוק)
- 7, Remote Flash
- שדרוג, 7
- ROM (זיכרון לקריאה בלבד)
- לא תקף, 8
- נורות מקלדת, טבלה, 9

S

- 41, Smart Cover Sensor (חיישן מכסה חכם)
- SSM (מנהל תוכנת המערכת), 6

ת

- תווי הפרדה של המקלדת, שפות שונות, 29
- תווי הפרדה, טבלה, 29
- תוכנה
- Drive Protection System (מערכת להגנה על כוננים), 48
- 8, ROM FailSafe Boot Block
- אבטחת רשומת אתחול ראשית, 45 עד 46
- בקרת נכסים, 21
- הודעות כשל והתאוששות, 48
- כלי העוזר Computer Setup (הגדרות מחשב) (F10)
- שילוב, 2
- תמונת תוכנה מותקנת מראש, 2
- תצורה התחלתית, 2
- תקליטון בר-אתחול, מידע חשוב, 47

A

- 6, ActiveUpdate
- 5, Altiris PC Transplant Pro
- 4, Altiris

D

- DiskOnKey
- בר-אתחול, 13 עד 18
- ראה גם HP Drive Key
- 41 עד 39, Drivelock

F

- 8, FailSafe Boot Block ROM

H

- 4, HP Client Manager
- HP Drive Key
- בר-אתחול, 13 עד 18
- ראה גם DiscOnKey

